Declaración de Prácticas de Confianza

Información general

Control documental

Clasificación de seguridad:	**Público**
Versión:	**1.2**
Fecha edición:	**03/04/2018**
Fichero:	**LGT_DPC v1r2.docx**
Formato:	**Word 2017**

Estado formal

Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: Astrea Fecha: 03/04/2018	Nombre: DG Fecha: 03/04/2018	Nombre: LOGALTY Fecha: 23/10/2018

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
1.0	Original	Creación del documento	Astrea / DG	03/04/2018
1.1	En general	Revisión RGPD Revisión después CAR 2018	Astrea	22/10/2018
1.2	1.5	Cambio denominación Social	DG	23/10/2018

Índice

INFORMACIÓN GENERAL 2

CONTROL DOCUMENTAL 2
ESTADO FORMAL 2
CONTROL DE VERSIONES 3

ÍNDICE 4

ACRONIMOS 9
DEFINICIONES 12

1 INTRODUCCIÓN 15

1.2.1 Identificadores de certificados 15
1.3.1 Prestador de servicios de certificación 16
1.3.2 Jerarquía de Logalty en desuso 18
1.3.3 Registradores 19
1.3.4 Entidades finales 20
1.3.5 Emisión de certificados de pruebas 22
1.4.1 Usos permitidos para los certificados 23
1.4.2 Límites y prohibiciones de uso de los certificados 42
1.5.1 Organización que administra el documento 43
1.5.2 Datos de contacto de la organización 43
1.5.3 Procedimientos de gestión del documento 44

2 PUBLICACIÓN DE INFORMACIÓN Y DEPÓSITO DE CERTIFICADOS 46

3 IDENTIFICACIÓN Y AUTENTICACIÓN 48

3.1.1 Tipos de nombres 48
3.1.2 Significado de los nombres 51
3.1.3 Empleo de anónimos y seudónimos 51
3.1.4 Interpretación de formatos de nombres 51
3.1.5 Unicidad de los nombres 52
3.1.6 Resolución de conflictos relativos a nombres 52
3.2.1 Prueba de posesión de clave privada 54
3.2.2 Autenticación de la identidad de una organización, empresa o entidad mediante representante 54
3.2.3 Autenticación de la identidad de una persona física 55
3.2.4 Identificación de la entidad en un certificado de autenticación web 57
3.2.5 Información de suscriptor no verificada 57
3.2.6 Autenticación de las Autoridades de Registro 58

4 REQUISITOS DE OPERACIÓN DEL CICLO DE VIDA DE LOS CERTIFICADOS 60

4.1.1 Legitimación para solicitar la emisión 60
4.1.2 Procedimiento de alta y responsabilidades 60
4.2.1 Ejecución de las funciones de identificación y autenticación 61
4.2.2 Aprobación o rechazo de la solicitud 61
4.2.3 Plazo para resolver la solicitud 62
4.3.1 Acciones de LOGALTY durante el proceso de emisión 62
4.3.2 Notificación de la emisión al suscriptor 63
4.4.1 Responsabilidades de la LOGALTY CA 63
4.4.2 Conducta que constituye aceptación del certificado 65
4.4.3 Publicación del certificado 65
4.4.4 Notificación de la emisión a terceros 65
4.5.1 Uso por el firmante 65
4.5.2 Uso por el suscriptor 66
4.5.3 Uso por el tercero que confía en certificados 68
4.8.1 Causas de revocación de certificados 70
4.8.2 Legitimación para solicitar la revocación 71
4.8.3 Procedimientos de solicitud de revocación 71
4.8.4 Plazo temporal de solicitud de revocación 72
4.8.5 Plazo temporal de procesamiento de la solicitud 73
4.8.6 Obligación de consulta de información de revocación de certificados 73
4.8.7 Frecuencia de emisión de listas de revocación de certificados (LRCs) 73
4.8.8 Plazo máximo de publicación de LRCs 73
4.8.9 Disponibilidad de servicios de comprobación en línea de estado de certificados 73
4.8.10 Obligación de consulta de servicios de comprobación de estado de certificados 74
4.8.11 Requisitos especiales en caso de compromiso de la clave privada 75
4.8.12 Causas de suspensión de certificados 75
4.8.13 Solicitud de suspensión 75
4.8.14 Procedimientos para la petición de suspensión 76
4.8.15 Período máximo de suspensión 76
4.10.1 Características operativas de los servicios 77
4.10.2 Disponibilidad de los servicios 77
4.10.3 Características opcionales 77
4.11.1 Política y prácticas de depósito y recuperación de claves 77
4.11.2 Política y prácticas de encapsulado y recuperación de claves de sesión 77

5 CONTROLES DE SEGURIDAD FÍSICA, DE GESTIÓN Y DE OPERACIONES 78

5.1.1 Localización y construcción de las instalaciones 78
5.1.2 Acceso físico 79
5.1.3 Electricidad y aire acondicionado 80
5.1.4 Exposición al agua 80
5.1.5 Prevención y protección de incendios 81
5.1.6 Almacenamiento de soportes 81

5.1.7 Tratamiento de residuos 81
5.1.8 Copia de respaldo fuera de las instalaciones 81
5.2.1 Funciones fiables 82
5.2.2 Número de personas por tarea 83
5.2.3 Identificación y autenticación para cada función 83
5.2.4 Roles que requieren separación de tareas 83
5.2.5 Sistema de gestión PKI 83
5.3.1 Requisitos de historial, calificaciones, experiencia y autorización 84
5.3.2 Procedimientos de investigación de historial 85
5.3.3 Requisitos de formación 85
5.3.4 Requisitos y frecuencia de actualización formativa 86
5.3.5 Secuencia y frecuencia de rotación laboral 86
5.3.6 Sanciones para acciones no autorizadas 86
5.3.7 Requisitos de contratación de profesionales 86
5.3.8 Suministro de documentación al personal 87
5.4.1 Tipos de eventos registrados 87
5.4.2 Frecuencia de tratamiento de registros de auditoría 89
5.4.3 Período de conservación de registros de auditoría 89
5.4.4 Protección de los registros de auditoría 89
5.4.5 Procedimientos de copia de respaldo 90
5.4.6 Localización del sistema de acumulación de registros de auditoría 90
5.4.7 Notificación del evento de auditoría al causante del evento 90
5.4.8 Análisis de vulnerabilidades 90
5.5.1 Tipos de registros archivados 91
5.5.2 Período de conservación de registros 92
5.5.3 Protección del archivo 92
5.5.4 Procedimientos de copia de respaldo 92
5.5.5 Requisitos de sellado de fecha y hora 92
5.5.6 Localización del sistema de archivo 93
5.5.7 Procedimientos de obtención y verificación de información de archivo 93
5.7.1 Procedimientos de gestión de incidencias y compromisos 94
5.7.2 Corrupción de recursos, aplicaciones o datos 94
5.7.3 Compromiso de la clave privada de la entidad 94
5.7.4 Continuidad del negocio después de un desastre 95

6 CONTROLES DE SEGURIDAD TÉCNICA 97

6.1.1 Generación del par de claves 97
6.1.2 Envío de la clave privada al firmante 98
6.1.3 Envío de la clave pública al emisor del certificado 98
6.1.4 Distribución de la clave pública del prestador de servicios de certificación 98
6.1.5 Tamaños de claves 99
6.1.6 Generación de parámetros de clave pública 99

6.1.7 Comprobación de calidad de parámetros de clave pública 99
6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo 99
6.1.9 Propósitos de uso de claves 99
6.2.1 Estándares de módulos criptográficos 100
6.2.2 Control por más de una persona (n de m) sobre la clave privada 100
6.2.3 Depósito de la clave privada 100
6.2.4 Copia de respaldo de la clave privada 100
6.2.5 Archivo de la clave privada 101
6.2.6 Introducción de la clave privada en el módulo criptográfico 101
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico 101
6.2.8 Método de activación de la clave privada 103
6.2.9 Método de desactivación de la clave privada 103
6.2.10 Método de destrucción de la clave privada 103
6.2.11 Clasificación de módulos criptográficos 103
6.3.1 Archivo de la clave pública 104
6.3.2 Períodos de utilización de las claves pública y privada 104
6.4.1 Generación e instalación de datos de activación 104
6.4.2 Protección de datos de activación 104
6.5.1 Requisitos técnicos específicos de seguridad informática 105
6.5.2 Evaluación del nivel de seguridad informática 106
6.6.1 Controles de desarrollo de sistemas 106
6.6.2 Controles de gestión de seguridad 106

7 PERFILES DE CERTIFICADOS Y LISTAS DE CERTIFICADOS REVOCADOS 111

7.1.1 Número de versión 111
7.1.2 Extensiones del certificado 111
7.1.3 Identificadores de objeto (OID) de los algoritmos 111
7.1.4 Formato de Nombres 111
7.1.5 Restricción de los nombres 112
7.1.6 Identificador de objeto (OID) de los tipos de certificados 112
7.2.1 Número de versión 112
7.2.2 Perfil de OCSP 112

8 AUDITORÍA DE CONFORMIDAD 113

9 REQUISITOS COMERCIALES Y LEGALES 116

9.1.1 Tarifa de emisión o renovación de certificados 116
9.1.2 Tarifa de acceso a certificados 116
9.1.3 Tarifa de acceso a información de estado de certificado 116
9.1.4 Tarifas de otros servicios 116
9.1.5 Política de reintegro 116
9.2.1 Cobertura de seguro 117
9.2.2 Otros activos 117

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados 117
9.3.1 Informaciones confidenciales 117
9.3.2 Informaciones no confidenciales 118
9.3.3 Divulgación de información de suspensión y revocación 119
9.3.4 Divulgación legal de información 119
9.3.5 Divulgación de información por petición de su titular 119
9.3.6 Otras circunstancias de divulgación de información 119
9.5.1 Propiedad de los certificados e información de revocación 120
9.5.2 Propiedad de la Declaración de prácticas de confianza 120
9.5.3 Propiedad de la información relativa a nombres 121
9.5.4 Propiedad de claves 121
9.6.1 Obligaciones de la Entidad de Certificación de LOGALTY 121
9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados 123
9.6.3 Rechazo de otras garantías 124
9.6.4 Limitación de responsabilidades 124
9.6.5 Cláusulas de indemnidad 124
9.6.6 Caso fortuito y fuerza mayor 125
9.6.7 Ley aplicable 125
9.6.8 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación 126
9.6.9 Cláusula de jurisdicción competente 126
9.6.10 Resolución de conflictos 126

ACRONIMOS

AC (*o también CA*)	*Certificate Authority* Autoridad de Certificación
AR (o también RA)	*Registration Authority* Autoridad de Registro
CPD	Centro de Proceso de Datos
CPS (o también DPC)	*Certification Practice Statement*. Declaración de Prácticas de Certificación
CRL (o tambien LRC)	*Certificate Revocation List.* Lista de certificados revocados
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DNI	Documento Nacional de Identidad
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
EV (para SSL)	*Extended Validation* Validación extendida, en certificados SSL.
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Módulo de seguridad en Hardware
IETF	*Internet Engineering Task Force*
NIF	Número de Identificación Fiscal
NTP	*Network Time Protocol* Protocolo de tiempo en red.
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier*. Identificador de objeto
PDS	*PKI Disclosure Statements* Texto de Divulgación de PKI.

PIN	*Personal Identification Number*. Número de identificación personal
PKI	*Public Key Infrastructure*. Infraestructura de clave pública
QSCD (o también DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Dispositivo cualificado de creación de firma/sellos
QCP	*Qualified Certificate Policy* Política de certificados cualificados
QCP-n	*Policy for EU qualified certificate issued to a natural person* Política de certificados cualificados para personas físicas.
QCP-l	*Policy for EU qualified certificate issued to a legal person* Política de certificados cualificados para personas jurídicas.
QCP-n-qscd	*Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD* Política de certificados cualificados para personas físicas con dispositivo cualificado de firma/sello
QCP-l-qscd	*Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD* Política de certificados cualificados para personas jurídicas con dispositivo cualificado de firma/sello
QCP-w	*Policy for EU qualified website certificate issued to a natural or a legal person and linking the website to that person* Política de certificados cualificados para autenticación de sitios web, emitidos a personas jurídicas o físicas.
RFC	*Request for Comments* Documento RFC
RSA	Rivest-Shimar-Adleman.

	Tipo de algoritmo de cifrado
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	*Transmission Control. Protocol/Internet Protocol*. Sistema de protocolos, definidos en el marco de la IEFT.
TSA	*Time Stamping Authority* Autoridad de Sellado de Tiempo Electrónico
TSU	*Time Stamping Unit* Unidad de Sellado de Tiempo.
UTC	*Coordinated Universal Time* Tiempo universal coordinado
VPN	*Virtual Private Network.* Red privada virtual

DEFINICIONES

Autoridad de Certificación	*Es la entidad responsable de la emisión y gestión de los certificados digitales.*
Autoridad de Registro	*Entidad responsable de la gestión de las solicitudes, identificación y registro de los solicitantes de un certificado. Puede formar parte de la Autoridad de Certificación o ser ajena.*
Certificado	*Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.*
Clave pública	*Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.*
Clave privada	*Valor matemático conocido únicamente por el Sujeto/Firmante y usado para la creación de una firma digital o el descifrado de datos.* *La clave privada de la AC será usada para la firma de certificados y firma de CRL's.* *La clave privada del servicio TSA será usada para la firma de los sellos de tiempo.*
CPS	*Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.*
CRL	*Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.*
Datos de Activación	*Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada*
DCCF	*Dispositivo Cualificado de creación de firma. Elemento software o hardware, convenientemente certificado, empleado por el Sujeto/Firmante para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Sujeto/Firmante.*

Firma digital	*El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera:* *a) que los datos no han sido modificados (integridad)* *b) que la persona que firma los datos es quien dice ser (identificación)* *c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)*
OID	*Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.*
Par de claves	*Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.*
PKI	*Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.*
Solicitante	*En el contexto de este documento, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de una persona jurídica, o de sí misma para certificados individuales.*
Suscriptor	*En el contexto de este documento la persona jurídica propietaria del certificado (a nivel corporativo) o la persona física en certificados individuales.*
Sujeto/Firmante	*En el contexto de este documento, la persona física cuya clave pública es certificada por la AC y dispone de, o tiene acceso de forma exclusiva a, una clave privada válida para generar firmas digitales.*
Parte Usuaria	*En el contexto de este documento, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado*
Emisor	*Aquella persona física o jurídica que pone a disposición de Logalty la documentación repecto de la cual Logalty presta sus servicios de Contratación online, Notificación certificada, Comunicación certificada o Grabación de Llamadas.*

Receptor	*Aquella persona jurídica o física a quien va destinada la documentación respecto de la cual Logalty presta sus servicios de Contratación online, Notificación certificada, Comunicación certificada o Grabación de Llamadas.*

1 Introducción

1.1 Presentación

Este documento declara las prácticas de certificación de firma electrónica de la Entidad de Certificación de Logalty.

Los tipos de certificados que se emiten son los siguientes:

- CERTIFICADOS CUALIFICADOS
  - De Persona Física
  - De Persona Física vinculada
  - De Persona Física Representante
  - De Sello electrónico de Persona Jurídica
  - De Autenticación Web
  - De Servicio de Sellado de Tiempo Electrónico

1.2 Nombre del documento e identificación

Este documento es la “Declaración de Prácticas de Confianza de LOGALTY”.

1.2.1 Identificadores de certificados

Logalty ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

OID	Tipos de certificados CUALIFICADOS
1.3.6.1.4.1.30210.1.1.1	De Persona Física en QSCD con gestión de claves centralizada
1.3.6.1.4.1.30210.1.1.2	De Persona Física sin QSCD con gestión de claves centralizada

1.3.6.1.4.1.30210.1.2.1	De Persona Física vinculada a Persona Jurídica en QSCD con gestión de claves centralizada
1.3.6.1.4.1.30210.1.2.2	De Persona Física vinculada a Persona Jurídica en software con gestión de claves centralizada
1.3.6.1.4.1.30210.1.2.3	De Persona Física vinculada a Persona Jurídica en software con gestión distribuida de claves
1.3.6.1.4.1.30210.1.3.1	De Sello electrónico de persona jurídica en QSCD con gestión de claves centralizada
1.3.6.1.4.1.30210.1.3.2	De Sello electrónico de persona jurídica en software con gestión de claves centralizada
1.3.6.1.4.1.30210.1.3.3	De Sello electrónico de persona jurídica en software con gestión distribuida de claves
1.3.6.1.4.1.30210.1.4.1	De Autenticación Web
1.3.6.1.4.1.30210.1.5.1	De Sello electrónico de TSA
1.3.6.1.4.1.30210.1.6.1	De Persona Física representante de Persona Jurídica ante las AAPP en QSCD con gestión de claves centralizada
1.3.6.1.4.1.30210.1.6.2	De Persona Física representante de Persona Jurídica ante las AAPP en software con gestión de claves centralizada
1.3.6.1.4.1.30210.1.7.1	De Persona Física representante de Entidad Sin Personalidad Jurídica ante las AAPP en QSCD con gestión de claves centralizada
1.3.6.1.4.1.30210.1.7.2	De Persona Física representante de Entidad Sin Personalidad Jurídica ante las AAPP en software con gestión de claves centralizada

En caso de contradicción entre esta Declaración de Prácticas de Confianza y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas.

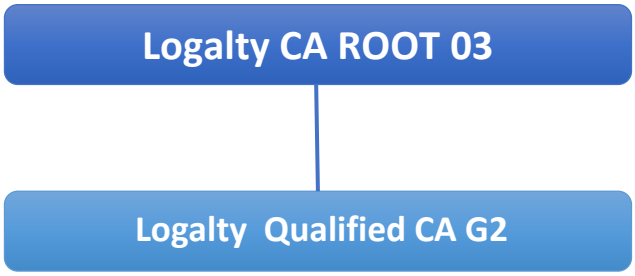
1.3 Participantes en los servicios de certificación

1.3.1 Prestador de servicios de certificación

El prestador de servicios de certificación es la persona, física o jurídica, que expide y gestiona certificados para entidades finales, empleando una Entidad de Certificación, o presta otros servicios relacionados con la firma electrónica.

LOGALTY es un prestador de servicios de certificación, que actúa de acuerdo con lo dispuesto en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para la transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE , y las normas técnicas del ETSI aplicables a la expedición y gestión de certificados cualificados, principalmente ETSI EN 319 401, ETSI EN 319 411-1 y ETSI EN 319 411-2, al objeto de facilitar el cumplimiento de los requisitos legales y el reconocimiento internacional de sus servicios.

Para la prestación de los servicios de certificación, LOGALTY ha establecido la siguiente jerarquía de entidades de certificación



1.3.1.1 Logalty CA ROOT 03

Se trata de la entidad de certificación raíz de la jerarquía que emite certificados a otras entidades de certificación, y cuyo certificado de clave pública ha sido autofirmado.

Datos de identificación:

CN:	Logalty CA ROOT 03
Huella digital:	5b39539340c50a9cb6f8bcf66a3e262c5f122f60
Válido desde:	6 de junio de 2018 12:17:11
Válido hasta:	6 de junio de 2043 12:17:11
Longitud de clave RSA:	4096 bits

1.3.1.2 Logalty Qualified CA G2

Se trata de la entidad de certificación dentro de la jerarquía que emite los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la Logalty CA ROOT 03.

Datos de identificación:

CN:	Logalty Qualified CA G2
Huella digital:	62a8cd2634595e26d72126a2b1df29175f9b0c17
Válido desde:	6 de junio de 2018 13:08:49
Válido hasta:	6 de junio de 2031 13:08:49
Longitud de clave RSA:	4096 bits

1.3.1.3 Plataforma de gestión NEBULA

Plataforma de gestión centralizada de certificados para los siguientes usos:

- Gestión de solicitudes y aprobaciones de certificados
- Gestión de peticiones de certificados
- Gestión de las solicitudes de renovación y revocación de certificados.

Esta plataforma utiliza un "nshield HSM Family" v.11.72.02 que se encuentra certificado conforme la ISO/IEC 15408 (Common Criteria) v.3.1 EAL4+ (AVA_VAN.5) como dispositivo cualificado de creación de firma o sello electrónico conforme al Reglamento (UE) 910/2014.

1.3.2 Jerarquía de Logalty en desuso

Jerarquía inicial de Logalty que ha sido renovada por la anteriormente descrita, por lo que ha pasado a estar en desuso.

1.3.2.1 Logalty CA ROOT 02

Se trata de la entidad de certificación raíz de la jerarquía que emitía certificados a otras entidades de certificación, y cuyo certificado de clave pública ha sido autofirmado.

Datos de identificación:

CN:	Logalty CA ROOT 02
Huella digital:	ce 51 d1 0f 6a eb 4b ae 1a 5e f3 35 62 cf 7b 53 a2 da fb e2
Válido desde:	25 de octubre de 2017 15:29:56
Válido hasta:	25 de octubre de 2042 15:29:56
Longitud de clave RSA:	4096 bits

1.3.2.2 Logalty Qualified CA G1

Se trata de la entidad de certificación dentro de la jerarquía que emitía los certificados a las entidades finales, y cuyo certificado de clave pública ha sido firmado digitalmente por la Logalty CA ROOT 02.

Datos de identificación:

CN:	Logalty Qualified CA G1
Huella digital:	9a 01 8b c7 13 ee 5d a6 1e 3d 34 44 f9 92 bb 8c ca 79 78 ef
Válido desde:	25 de octubre de 2017 15:46:41
Válido hasta:	25 de octubre de 2030 15:46:41
Longitud de clave RSA:	4096 bits

1.3.3 Registradores

En general, el prestador del servicio de certificación actúa como registrador de la identidad de los suscriptores de certificados.

También son registradores de los certificados sujetos a esta Declaración de Prácticas de Confianza, en aquellos tipos de certificados que dispongan de la condición de corporativos, las unidades designadas para esta función por los suscriptores de los certificados, como un

departamento de personal, dado que disponen de los registros auténticos acerca de la vinculación de los firmantes con el suscriptor.

También son registradores de los certificados sujetos a esta Declaración de Prácticas de Confianza destinados a los receptores, los operadores de la una organización contratada por Logalty, y bajo su responsabilidad, para realizar el procedimiento de registro presencial.

Las funciones de registro de los suscriptores se realizan por delegación y de acuerdo con las instrucciones del prestador de servicios de certificación, en los términos del artículo 24.1 del Reglamento EU 910/2014, y bajo la plena responsabilidad del prestador de servicios de confianza frente a terceros.

1.3.4 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de identificación y firma electrónica.

Serán entidades finales de los servicios de certificación de Logalty las siguientes:

1. Suscriptores del servicio de certificación.
2. Firmantes.
3. Partes usuarias.

1.3.4.1 Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son:

- las empresas, entidades u organizaciones que los adquieren a LOGALTY para su uso en su ámbito corporativo empresarial u organizativo, y se encuentran identificados en los certificados,
- las personas físicas que los adquieren a LOGALTY para su uso, principalmente, en relación con los servicios de notificación y comunicación de LOGALTY, y se encuentran identificados en los certificados.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, para su uso propio – certificados de sello electrónico –, o al objeto de facilitar la certificación de la identidad de una persona concreta debidamente autorizada para diversas actuaciones en el

ámbito organizativo del suscriptor – certificados de firma electrónica. En este último caso, esta persona figura identificada en el certificado, según se dispone en el epígrafe siguiente.

El suscriptor del servicio de certificación es, por tanto, el cliente del prestador de servicios de certificación, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por el prestador del servicio de certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados, en especial ETSI EN 319 411-2, secciones 5.4.2 y 6.3.4).

1.3.4.2 Firmantes

Los firmantes son las personas físicas que poseen de forma exclusiva (o tienen bajo su exclusivo control) las claves de firma digital para identificación y firma electrónica avanzada o cualificada; siendo típicamente los empleados, clientes y otras personas vinculadas a los suscriptores, en los certificados de persona física.

Los firmantes se encuentran debidamente autorizados por el suscriptor y debidamente identificados en el certificado mediante su nombre y apellidos, y número de identificación fiscal válido en la jurisdicción de expedición del certificado, sin que sea posible, en general, el empleo de seudónimos.

La clave privada de un firmante, no puede ser recuperada por el prestador de servicios de certificación.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la identificación, también se emplea el término más genérico de “persona física identificada en el certificado”, siempre con pleno respeto al cumplimiento de la legislación de firma electrónica en relación con los derechos y obligaciones del firmante.

1.3.4.3 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas digitales, sellos electrónicos y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de confianza y en las correspondientes instrucciones disponibles en la página web de LOGALTY (https://www.logalty.es/certificateauthority/)

1.3.5 Emisión de certificados de pruebas

LOGALTY emite certificados de pruebas para su revisión en procesos de inspección o notificación por el Supervisor y en procesos de evaluación en auditorías de conformidad. Estos certificados emitidos bajo la jerarquía en producción de LOGALTY incluye datos ficticios que son:

Certificados de Personas Físicas	
Nombre	Pruebas
Primer Apellido	Perez
Segundo Apellido	Perez
DNI/NIE	01234567L

Certificados de Sello Electrónico	
Campo O	Organization Prueba
SerialNumber	01234567L
Locality	Alcobendas
OU	Operaciones

Para poder disponer de estos certificados se debe enviar un correo electrónico a la dirección info.ca@logalty.com

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1 Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, visibles en el web de LOGALTY (https://www.logalty.es/certificateauthority/)

1.4.1.1 Certificado cualificado de Persona Física en QSCD con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.1.1
De acuerdo con la política QCP-n-qscd	0.4.0.194112.1.2

Los certificados de persona física emitidos en QSCD, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados de persona física emitido en QSCD, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del firmante y permiten la generación de la "**firma electrónica cualificada**"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" describe el uso de este certificado.

1.4.1.2 Certificado cualificado de Persona Física en software con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.1.2
De acuerdo con la política QCP-n	0.4.0.194112.1.0

Los certificados de persona física emitidos en software, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento

Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo seguro de creación de firma.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del firmante y permiten la generación de la "**firma electrónica avanzada"** basada en certificado electrónico cualificado.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    - Firma digital (para realizar la función de autenticación)
    - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

d) El campo "User Notice" describe el uso de este certificado.

1.4.1.3 Certificado cualificado de Persona Física vinculada a Persona Jurídica en QSCD con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.2.1
De acuerdo con la política QCP-n-qscd	0.4.0.194112.1.2

Los certificados de persona física vinculada emitidos en QSCD, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Los certificados de persona física vinculada emitido en QSCD, funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permiten la generación de la "**firma electrónica cualificada**"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" describe el uso de este certificado.

1.4.1.4 Certificado cualificado de Persona Física vinculada a Persona Jurídica en software con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.2.2
De acuerdo con la política QCP-n	0.4.0.194112.1.0

Los certificados de persona física vinculada emitidos en software, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo seguro de creación de firma.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permiten la generación de la "**firma electrónica avanzada"** basada en certificado electrónico cualificado.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

d) El campo "User Notice" describe el uso de este certificado.

1.4.1.5 Certificado cualificado de Persona Física vinculada a Persona Jurídica en software con gestión distribuida de claves

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.2.3
De acuerdo con la política QCP-n	0.4.0.194112.1.0

Los certificados de persona física vinculada emitidos en software, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con dispositivo seguro de creación de firma.

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

Estos certificados garantizan la identidad del firmante y su vinculación con el suscriptor del servicio de certificación, y permiten la generación de la "**firma electrónica avanzada"** basada en certificado electrónico cualificado.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    - Firma digital (para realizar la función de autenticación)
    - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

d) El campo “User Notice” describe el uso de este certificado.

1.4.1.6 Certificado cualificado de Sello electrónico de persona jurídica en QSCD con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.3.1
De acuerdo con la política QCP-l-qscd	0.4.0.194112.1.3

Los certificados centralizados de sello electrónico de persona jurídica emitidos en QSCD, son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor del servicio de certificación, y permiten la generación del “**sello electrónico cualificado**”; es decir, el sello electrónico avanzado que se basa en un certificado cualificado y que ha sido generado empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 35.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, disfrutará de la presunción de integridad de los datos y de la corrección del origen de los datos a los que el sello electrónico cualificado esté vinculado.

En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

c) El campo “User Notice” describe el uso de este certificado.

1.4.1.7 Certificado cualificado de Sello electrónico de persona jurídica en software con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.3.2
De acuerdo con la política QCP-l	0.4.0.194112.1.1

Los certificados centralizados de sello electrónico de persona jurídica, son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados **no funcionan** con dispositivo cualificado de creación de firma.

Estos certificados son gestionados de forma centralizada.

En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo “Qualified Certificate Statements” **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

d) El campo “User Notice” describe el uso de este certificado.

1.4.1.8 Certificado cualificado de Sello electrónico de persona jurídica en software con gestión distribuida de claves

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.3.3
De acuerdo con la política QCP-l	0.4.0.194112.1.1

Los certificados distribuidos de sello electrónico de persona jurídica, son certificados cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados **no funcionan** con dispositivo cualificado de creación de firma.

Estos certificados son gestionados de forma distribuida sin la participación de una herramienta de gestión centralizada.

En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

e) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)

- Compromiso con el contenido (para realizar la función de firma electrónica)

f) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

g) En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

h) El campo "User Notice" describe el uso de este certificado.

1.4.1.9 Certificado cualificado de Autenticación Web

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.4.1
De acuerdo con la política QCP-w	0.4.0.194112.1.4
De acuerdo con CAB FORUM – SSL EV	2.23.140.1.1

Los certificados de autenticación web, son certificados cualificados de acuerdo con el artículo 45 y con el Anexo IV del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados se emiten a direcciones web para la identificación y el establecimiento de canales seguros entre el navegador de un usuario (verificador) y el servidor web del titular de este certificado. Cumple los requisitos del Guidelines for Issuance and Management of extended validation certificates del CA/BROWSER FORUM (http://www.cabforum.og).

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto permite realizar, las siguientes funciones:

   a. Digital Signature (para la función de autenticación)
   b. Key Encipherment (para la gestión y transporte de claves)

b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo “User Notice” describe el uso de este certificado.

1.4.1.10 Certificado cualificado de Sello electrónico para Servicio de Sellado de Tiempo

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.5.1
De acuerdo con la política QCP-l	0.4.0.194112.1.1

Los certificados de sello electrónico de TSA/TSU son certificados cualificados de acuerdo con el artículo 38 y el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 421 y ETSI EN 319 422.

Este certificado permite a Unidades de Sellado de Tiempo o TSU emitir los sellos de tiempo cuando reciben una solicitud bajo las especificaciones de la RFC3161.

Las claves se generan en soporte de un dispositivo cualificado (QSCD).

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo “key usage” tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

a. Content Commitment

b) El campo “extend key usage” tiene activada la función:
   a. TimeStamping

c) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
   a. QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

d) El campo “User Notice” describe el uso de este certificado.

1.4.1.11 Certificado cualificado de Persona Física REPRESENTANTE de Persona Jurídica ante las AAPP, en QSCD con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.6.1
De acuerdo con la política QCP-n-qscd	0.4.0.194112.1.2
De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas	2.16.724.1.3.5.8

Estos certificados, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son certificados de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor y el firmante, indican una relación de representación legal o apoderamiento general entre el firmante y una entidad, empresa u

organización descrita en el campo "O" (Organization), y permiten la generación de la "**firma electrónica cualificada**"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

Este certificado incluye un campo (Description) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que represente y, en caso de ser obligatoria, la inscripción de los datos registrales.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    - Firma digital (para realizar la función de autenticación)
    - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" describe el uso de este certificado.

1.4.1.12 Certificado cualificado de Persona Física REPRESENTANTE de Persona Jurídica ante las AAPP, en software con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.6.2
De acuerdo con la política QCP-n	0.4.0.194112.1.0
De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas	2.16.724.1.3.5.8

Estos certificados, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con un dispositivo cualificado de creación de firma.

Estos certificados son certificados de representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor y el firmante, indican una relación de representación legal o apoderamiento general entre el firmante y una entidad, empresa u organización descrita en el campo "O" (Organization), y permiten la generación de la "**firma electrónica avanzada**" basada en un certificado electrónico cualificado.

Este certificado incluye un campo (Description) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad a la que represente y, en caso de ser obligatoria, la inscripción de los datos registrales.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado..

d) El campo "User Notice" describe el uso de este certificado.

1.4.1.13 Certificado cualificado de Persona Física REPRESENTANTE de Entidad Sin Personalidad Jurídica ante las AAPP, en QSCD con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.7.1
De acuerdo con la política QCP-n-qscd	0.4.0.194112.1.2
De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas	2.16.724.1.3.5.9

Estos certificados, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados son certificados de representante de entidad sin personalidad jurídica, en el que el Representante tiene plenas capacidades para actuar en nombre de la Entidad sin Personalidad Jurídica ante las Administraciones Públicas[1].

Este certificado incluye un campo (Description) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad sin personalidad jurídica a la que represente y, en caso de ser obligatoria, la inscripción de los datos registrales.

Estos certificados son gestionados de forma centralizada.

Estos certificados garantizan la identidad del suscriptor y el firmante, indican una relación de representación legal o apoderamiento general entre el firmante y una entidad sin personalidad jurídica descrita en el campo "O" (Organization), y permiten la generación de la "**firma electrónica cualificada**"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendá un efecto jurídico equivalente al de una fima manuscrita.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

[1] De acuerdo con el punto 14.1.3.1 del documento "Perfiles de Certificados Electrónicos" del Ministerio de Hacienda y Administraciones Públicas (abril 2016)

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" describe el uso de este certificado.

1.4.1.14 Certificado cualificado de Persona Física REPRESENTANTE de Entidad sin Personalidad Jurídica ante las AAPP, en software con gestión de claves centralizada

Este certificado dispone de los siguientes OID:

En la jerarquía de certificación de Logalty	1.3.6.1.4.1.30210.1.7.2
De acuerdo con la política QCP-n	0.4.0.194112.1.0
De acuerdo con los perfiles de certificados del Ministerio de Hacienda y Administraciones Públicas	2.16.724.1.3.5.9

Estos certificados, son certificados cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

Estos certificados no funcionan con un dispositivo cualificado de creación de firma.

Estos certificados son certificados de representante de entidad sin personalidad jurídica, en el que el Representante tiene plenas capacidades para actuar en nombre de la Entidad sin Personalidad Jurídica ante las Administraciones Públicas[2].

Estos certificados son gestionados de forma centralizada.

Este certificado incluye un campo (Description) en el Subject donde se indica el documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad sin personalidad jurídica a la que represente y, en caso de ser obligatoria, la inscripción de los datos registrales.

Estos certificados garantizan la identidad del suscriptor y el firmante, indican una relación de representación legal o apoderamiento general entre el firmante y una entidad sin personalidad jurídica descrita en el campo "O" (Organization), y permiten la generación de la "**firma electrónica avanzada**" basada en un certificado electrónico cualificado.

También se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) Otras aplicaciones de firma digital.

Estos certificados no permiten el cifrado de documentos, contenidos ni mensajes de datos. En todo caso, LOGALTY no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto permite realizar, las siguientes funciones:
    - Firma digital (para realizar la función de autenticación)
    - Compromiso con el contenido (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:

[2] De acuerdo con el punto 14.1.3.1 del documento "Perfiles de Certificados Electrónicos" del Ministerio de Hacienda y Administraciones Públicas (abril 2016)

- QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) En el campo "Qualified Certificate Statements" **no aparece** la declaración QcSSCD (0.4.0.1862.1.4), ya que este certificado no se usa con un dispositivo cualificado.

d) El campo "User Notice" describe el uso de este certificado.

1.4.2 Límites y prohibiciones de uso de los certificados

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Del mismo modo, los certificados deben emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de Logalty (https://www.logalty.es/certificateauthority/)

El empleo de los certificados digitales en operaciones que contravienen esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos con las entidades de registro o con sus firmantes/suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a LOGALTY, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

LOGALTY no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de LOGALTY emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor, al firmante o a la persona responsable de la custodia, cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en esta DPC, los documentos jurídicos vinculantes con cada certificado, o los contratos o convenios con las entidades de registro o con sus suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

1.5 Administración de la política

1.5.1 Organización que administra el documento

Logalty Trust Services

Logalty Servicios de Tercero de Confianza SL

Avenida de la Industria, 49

28108 Alcobendas, Madrid

España

Phone: +34 902 78 99 74

Email: info.ca@logalty.com

1.5.2 Datos de contacto de la organización

Logalty Servicios de Tercero de Confianza SL

Avenida de la Industria, 49

28108 Alcobendas, Madrid (España)

Phone: +34 915 145 800

Fax: +34 917 913 085

Email: logalty@logalty.com

Identificación Registro	Registro Mercantil de Madrid
Tomo	22055
Folio	60
Hoja	M-393315
CIF	B-84492891

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de LOGALTY garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

1.5.3.1 Revisión del documento

Logalty revisa esta DPC una vez al año como mínimo.

El Responsable de Seguridad será el responsable del mantenimiento de este documento siguiendo las directrices de la Política de Seguridad[3] y del Procedimiento de Mejora Continua[4] de Logalty.

El Responsable de Seguridad propone cambios y recoge sugerencias y propuestas para su estudio y envío al Comité de Riesgos y de Seguridad de la Información para su aprobación.

El Comité de Riesgos y de Seguridad avaluará la necesidad que los cambios propuestos requieran de notificación ante al supervisor.

Fases de seguimiento de los cambios:

- Fase A: Recogida de sugerencias y propuestas
- Fase B: Estudio, análisis, comprobación y redacción
- Fase C: Envío al Comité de Riesgos y de Seguridad de la Información para comentarios, redacción final y aprobación.

[3] Documento: LSGSIPO008 - Política de seguridad

[4] Documento: LSGSIPR012 - Procedimiento de Mejora Continua

- Fase D: Publicación en la web, y si fuera requerido notificación al supervisor.

Logalty realiza una nueva revisión de esta DPC ante la inclusión de cambios suficientemente relevantes para la gestión de los servicios de certificación. La descripción de los cambios se incluirán en el apartado “control de versiones” de la sección “Información General” en el inicio de este documento.

1.5.3.2 Aprobación del documento

Las modificaciones futuras de esta Declaración de Prácticas de Confianza, de la Política de Seguridad y de los Textos de Divulgación (PDS) son aprobadas por el Comité de Riesgos y de Seguridad de la Información, el cuál de forma adicional se responsabilizará de su correcta implementación.

LOGALTY comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://www.logalty.es/certificateauthority.

2 Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

LOGALTY dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de LOGALTY, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de prácticas de confianza.

2.2 Publicación de información del prestador de servicios de certificación

LOGALTY publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona física identificada en el certificado.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- La Declaración de prácticas de confianza.
- Los textos de divulgación (PKI Disclosure Statements - PDS), como mínimo en lengua inglesa.

2.3 Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las PDS y la Declaración de prácticas de confianza, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de prácticas de confianza se rigen por lo establecido en la sección 1.5 de este documento.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de esta Declaración de Prácticas de Confianza.

2.4 Control de acceso

LOGALTY no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

LOGALTY emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Identificación y autenticación

3.1 Registro inicial

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1 Certificados de persona física

Country [C]	Ej: "ES" (o el correspondiente al país del suscriptor)
Surname	Apellidos
Given Name	Nombre
Serial Number	DNI/NIE (en formato ETSI EN 319412-1)
Common Name (CN)	Nombre, apellidos y número de la persona física

3.1.1.2 Certificados de persona física vinculada

Country [C]	Ej: "ES" (o el correspondiente al país del suscriptor)
Organization (O)	Organización a la que se encuentra vinculado el firmante

Organizational Unit (OU)	Departamento en la Organización a la que se encuentra vinculado el firmante u otra información sobre la Organización
Organizationidentifier	NIF de la persona jurídica a la que está vinculado (en formato ETSI EN 319412-1)
Surname	Apellidos
Given Name	Nombre
Title	Cargo / otros
Serial Number	DNI/NIE (en formato ETSI EN 319412-1)
Common Name (CN)	Nombre, apellidos y número de la persona física

3.1.1.3 Certificados de persona física representante de persona jurídica

Country [C]	Ej: “ES” (o el correspondiente al país del suscriptor)
Organization (O)	Organización de la que es representante
Organizational Unit (OU)	Departamento en la Organización de la que es representante el firmante u otra información sobre la Organización
Organizationidentifier	NIF de la persona jurídica a la que está vinculado (en formato ETSI EN 319412-1)
Surname	Apellidos
Given Name	Nombre
Title	Cargo / otros
Serial Number	DNI/NIE (en formato ETSI EN 319412-1)

Common Name (CN)	Nombre, apellidos y número de la persona física, así como el CIF de la persona jurídica subscriptora
Description	Documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la persona jurídica

3.1.1.4 Certificados de persona física representante de entidad sin personalidad jurídica

Country [C]	Ej: "ES" (o el correspondiente al país del suscriptor)
Organization (O)	Organización de la que es representante
Organizational Unit (OU)	Departamento en la Organización de la que es representante el firmante u otra información sobre la Organización
Organizationidentifier	NIF de la entidad sin personalidad jurídica a la que está vinculado (en formato ETSI EN 319412-1)
Surname	Apellidos
Given Name	Nombre
Title	Cargo / otros
Serial Number	DNI/NIE (en formato ETSI EN 319412-1)
Common Name (CN)	Nombre, apellidos y número de la persona física, así como el CIF de la entidad sin personalidad jurídica subscriptora
Description	Documento público que acredita de forma fehaciente las facultades del firmante para actuar en nombre de la entidad sin personalidad jurídica

3.1.1.5 Certificados de sello electrónico de persona jurídica

Country [C]	"ES"
Organization (O)	Nombre oficial de la persona jurídica
organizationIdentifier	NIF de la persona jurídica a la que está vinculado este sello (en formato ETSI EN 319412-1)
Serial Number	DNI de la persona jurídica
Locality	Localidad de la organización
Common Name	Nombre de la plataforma donde reside el sello

3.1.2 Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural, de acuerdo con lo establecido en la sección anterior.

3.1.3 Empleo de anónimos y seudónimos

En ningún caso se pueden utilizar seudónimos para identificar una entidad/empresa/organización, ni a un firmante.

En ningún caso se emiten certificados anónimos.

3.1.4 Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la legislación del país de establecimiento del suscriptor, en sus propios términos.

El campo “país” será el del país del subscriptor.

En los certificados de “*persona física vinculada*” muestra la relación entre una persona física y la empresa, entidad u organización con la que está vinculada, con independencia de la nacionalidad de la persona física. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor la entidad, empresa u organización, y la persona física vinculada la persona autorizada a su uso.

En los certificados emitidos a suscriptores españoles, el campo “*número de serie*” debe incluir el NIF del firmante, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de LOGALTY.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se debe producir, gracias a la presencia del número del Documento Nacional de Identidad, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) u otro identificador legalmente válido de la persona física.
- Cuando exista, Número de Identificación Fiscal (NIF) u otro identificador legalmente válido del suscriptor.
- Tipo de Certificado (Campo descripción del certificado).

3.1.6 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

LOGALTY no estará obligada a determinar previamente que un solicitante de certificados tiene derechos de propiedad industrial sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación del país del suscriptor, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

3.2 Validación inicial de la identidad

La identidad de los suscriptores de certificados resulta fijada en el momento de la firma del contrato entre LOGALTY y el suscriptor, cuando se verifica la existencia del suscriptor con la presentación de su documento nacional de identidad o similar y, cuando sea necesario, las escrituras correspondientes, , y los poderes de actuación de la persona que lo representa. Para esta verificación, se podrá emplear documentación pública o notarial, o la consulta directa a los registros públicos correspondientes.

En el caso de las personas físicas individuales, no vinculadas a un subscriptor corporativo, sus identidades se validan mediante la identificación por un operador autorizado por la Entidad de Registro y LOGALTY. En relación a dichos datos, Logalty **adquiere la condición de responsable del tratamiento** de conformidad con lo indicado en el RGPD.

En el caso de las personas físicas vinculadas a un subscriptor corporativo, sus identidades se validarán mediante los registros corporativos de la entidad, empresa u organización de derecho público o privado, suscriptoras de los certificados. El suscriptor producirá una

certificación de los datos necesarios, y la remitirá a LOGALTY, por los medios que ésta habilite, para el registro de la identidad de los firmantes.

En relación a los datos personales de cada entidad, empresa u organización de derecho público o privado **actúa como encargado del tratamiento** en los términos indicados en al apartado 9.4 de este documento.

3.2.1 Prueba de posesión de clave privada

La posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado por el suscriptor, en certificados de sello electrónico y de autenticación web, o por el firmante, en certificados de firma.

3.2.2 Autenticación de la identidad de una organización, empresa o entidad mediante representante

Las personas físicas con capacidad de actuar en nombre de las personas públicas o privadas suscriptoras, podrán actuar como representantes de las mismas, siempre y cuando exista una situación previa de representación legal o voluntaria entre la persona física y la persona pública o privada, que exige su reconocimiento por LOGALTY, la cual se realizará mediante el siguiente procedimiento presencial:

1. El representante del suscriptor se reunirá presencialmente con un representante autorizado de LOGALTY, el cual pondrá a su disposición un formulario de autenticación. Alternativamente, el representante del suscriptor podrá obtener el formulario de la página web de LOGALTY para su cumplimentación previa.

2. El representante cumplimentará el formulario, con las siguientes informaciones y a la que acompañará los siguientes documentos:
    - Sus datos de identificación como representante:
        - Nombre y apellidos.
        - Lugar y fecha de nacimiento.
        - Documento: DNI o NIF del representante.
    - Los datos de identificación del suscriptor al que representa:
        - Denominación o razón social.

- Toda información de registro existente, incluyendo los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante.
- Documento: NIF de la persona pública o privada.
- Documento: Documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

- Los datos relativos a la representación o la capacidad de actuación que ostenta:
  - La vigencia de la representación o la capacidad de actuación (fecha de inicio y fin).
  - La indicación de Representación o capacidad total. Esta comprobación se podrá realizar mediante consulta telemática al registro público donde conste inscrita la representación.

3. Cumplimentado y firmado el formulario, se firmará y entregará a LOGALTY junto con la documentación justificativa indicada.
4. El personal de LOGALTY comprobará la identidad del representante mediante la presentación del DNI o NIF, así como el contenido de la representación con la documentación.
5. Alternativamente, de acuerdo con lo establecido en el artículo 24.1 REGLAMENTO (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014, y en el artículo 13.1 de la Ley 59/2003, de 19 de diciembre, se podrá legitimar notarialmente la firma del formulario, y hacerse llegar a LOGALTY por correo postal certificado, en cuyo caso los pasos 3 a 4 anteriores no serán precisos.

La prestación del servicio de certificación digital se formaliza mediante el oportuno contrato entre LOGALTY y el suscriptor, debidamente representado.

3.2.3 Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1 En los certificados

La información de identificación de las personas físicas identificadas en los certificados cuyo subscriptor sea una persona jurídica se valida comparando la información de la solicitud con los registros de la entidad, empresa u organización de derecho público o privado a la que está vinculado, asegurando la corrección de la información a certificar.

La identidad de las personas físicas identificados en los certificados cuyo suscriptor sea esta misma persona física, se valida mediante la presentación de su documento oficial de identificación (Documento Nacional de Identidad, tarjeta de identidad, pasaporte u otro medio idóneo reconocido en derecho para su identificación).

3.2.3.2 Necesidad de presencia personal

En la solicitud de certificados de persona física cuyo subscriptor sea esta misma persona física, LOGALTY valida esta identidad, personándose la persona física y exhibiendo su documento oficial de identidad o similar ante un operador de una Autoridad de Registro autorizada por LOGALTY.

Para la solicitud de los certificados de persona física vinculada no se requiere la presencia física directa debido a la relación ya acreditada entre la persona física y entidad, empresa u organización de derecho público o privado a la que está vinculada.

Sin embargo, antes de la entrega de un certificado, la entidad, empresa u organización de derecho público o privado suscriptora, por medio de su responsable de certificación, de tenerlo, u otro miembro designado, deberá contrastar la identidad de la persona física identificada en el certificado mediante su presencia física.

Durante este trámite se confirma rigurosamente la identidad de la persona física identificada en el certificado.

Por este motivo, en todos los casos en que se expide un certificado se verifica presencialmente la identidad de la persona física firmante.

La Autoridad de Registro verificará mediante la exhibición de documentos o a través de sus propias fuentes de información, el resto de datos y atributos a incluir en el certificado, guardando documentación acreditativa de la validez de estos.

3.2.3.3 Vinculación de la persona física

La justificación documental de la vinculación de una persona física identificada en un certificado con la entidad, empresa u organización de derecho público o privado viene dada por su constancia en los registros internos (contrato de trabajo como empleado, o el contrato mercantil que lo vincula, o el acta donde se indique su cargo, o la solicitud como miembro de la organización…) de cada una de las personas públicas y privadas a las que están vinculadas.

3.2.4 Identificación de la entidad en un certificado de autenticación web

LOGALTY comprueba la existencia de la entidad solicitante de un certificado de autenticación web mediante el acceso a registros públicos (informa.es) o a la Agencia Tributaria (agenciatributaria.es).

LOGALTY comprueba la actividad operativa de la entidad accediendo a los registros de actividad empresarial.

LOGALTY de acuerdo con las guías de emisión de estos certificados con validación extendida verifica la exactitud de la solicitud del certificado, realizado por el solicitante marcando la casilla correspondiente, diferenciando los tipos de organización existentes como “privadas, “ gobierno”, “negocio” o “no comerciales”.

El procedimiento ampliado se indica en el documento: LGT_provisionCERT_emisor_distribuidos-SSL

3.2.5 Información de suscriptor no verificada

LOGALTY no incluye ninguna información de suscriptor no verificada en los certificados.

3.2.6 Autenticación de las Autoridades de Registro

LOGALTY realiza las verificaciones necesarias para confirmar la existencia de la organización que desea convertirse en Autoridad de Registro. LOGALTY obtiene la documentación de la organización que se presenta, además de utilizar sus propias fuentes de información.

LOGALTY, verifica y valida la identidad de los operadores de la Autoridad de Registro con la información que le remite el subscriptor, en la que incluye su autorización para actuar como tal.

LOGALTY se asegura que los operadores de la Autoridad de Registro reciban la formación suficiente para el desempeño de sus funciones, que verificará en las evaluaciones correspondientes.

Los operadores y responsables de certificación se autentican siempre con certificados digitales para la prestación de sus servicios ante la Autoridad de Registro.

3.3 Identificación y autenticación de solicitudes de renovación

Logalty no realiza renovaciones de certificados.

Antes de la caducidad del certificado se avisa al suscriptor para la emisión de un nuevo certificado, usando para ello las indicaciones del apartado 3.2 de esta DPC.

3.4 Identificación y autenticación de la solicitud de revocación

LOGALTY o una Entidad de Registro autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor o de la persona física identificada en el certificado, por medio de la plataforma electrónica NEBULA, de gestión del ciclo de vida de los certificados.
- El envío de una solicitud de revocación por parte del suscriptor o de la persona física identificada en el certificado, firmada electrónicamente.
- El uso de información que sólo conoce la persona física identificada en el certificado, y que le permite revocar de forma automática su certificado.
- La personación física en una oficina de la empresa, entidad u Organización subscriptora.
- Otros medios de comunicación, como el envío de la solicitud de revocación firmada manuscritamente junto a una fotocopia de su documento oficial de identificación, por medio de envío postal. Logalty realiza las comprobaciones pertinentes para asegurarse de la veracidad de la solicitud.

Ampliación del procedimiento en el documento: LGT_revocacionCERT

3.5 Autenticación de una petición de suspensión

Logalty no realiza suspensión de certificados.

4 Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud de emisión de certificado

4.1.1 Legitimación para solicitar la emisión

El solicitante del certificado, sea persona física o jurídica, debe firmar un contrato de prestación de servicios de certificación con LOGALTY.

Asimismo, con anterioridad a la emisión y entrega de un certificado, debe existir una solicitud de certificados en un documento específico de hoja de solicitud de certificados, que podrá ser en formato electrónico por medio de la plataforma electrónica existente.

Cuando el solicitante es una persona distinta al suscriptor, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por dicho solicitante en nombre propio para certificados en los que el subscriptor sea una persona física, o bien en nombre de la entidad, empresa u organización de derecho público o privado, que podrá ser en formato electrónico por medio de la plataforma electrónica existente.

4.1.2 Procedimiento de alta y responsabilidades

LOGALTY recibe solicitudes de certificados, realizadas a nombre de personas físicas, entidades, empresas u organizaciones de derecho público o privado.

Las solicitudes se instrumentan mediante un documento, cumplimentado por el solicitante a nombre de la persona física, entidad, empresa u organización de derecho público o privado, cuyo destinatario es LOGALTY, el cual incluirá los datos de las personas a las que se expedirán certificados. Esta solicitud puede ser realizada por medio de la plataforma electrónica existente. La solicitud, para certificados cuyo subscriptor será una persona jurídica, es realizada por el operador autorizado por el suscriptor (responsable de certificación) y que ha sido identificado en el contrato entre este suscriptor y LOGALTY.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3. También se deberá acompañar una dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, LOGALTY se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, LOGALTY verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud debe ser conservada y debidamente registrada y con garantías de seguridad e integridad durante **el plazo de 15 años desde la expiración del certificado**, incluso en caso de pérdida anticipada de vigencia por revocación. Esta documentación podrá ser conservada de forma segura por medio de la plataforma electrónica existente.

4.2.2 Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, LOGALTY debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Entidad de Certificación o de los suscriptores, LOGALTY denegará la petición, o detendrá su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso de que las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, LOGALTY denegará la solicitud definitivamente.

LOGALTY notifica al solicitante la aprobación o denegación de la solicitud.

LOGALTY podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes, por medio de la plataforma electrónica existente.

4.2.3 Plazo para resolver la solicitud

LOGALTY atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el contrato de emisión de certificados.

Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3 Emisión del certificado

4.3.1 Acciones de LOGALTY durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación, por medio de la plataforma electrónica existente.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que la misma implica la emisión de un nuevo certificado.

Durante el proceso, LOGALTY:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el Anexo I del Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1.
- Indica la fecha y la hora en que se expidió un certificado.

4.3.2 Notificación de la emisión al suscriptor

LOGALTY notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades de la LOGALTY CA

Durante este proceso, LOGALTY debe realizar las siguientes actuaciones:

- Cuando no se ha realizado con anterioridad, acreditar definitivamente la identidad de la persona física identificada en el certificado, con la colaboración del subscriptor (empresa, entidad u organización) y/o Autoridad de Registro, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Entregar a la persona física identificada en el certificado con la colaboración del Operador autorizado de la Autoridad de Registro, en el caso del subscriptor "receptor":
    - Las condiciones generales de prestación de servicios de certificación electrónica que incluye aviso legal sobre protección de datos, en formato papel.
    - Las indicaciones exactas para la aceptación del certificado accediendo a la plataforma electrónica Nébula, también en formato papel.
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de

certificación y de la Declaración de prácticas de confianza aplicable, como sus obligaciones, facultades y responsabilidades
    - Información acerca del certificado.
    - Reconocimiento, por parte del firmante, de disponer de acceso al certificado.
    - Régimen de obligaciones del firmante.
    - Responsabilidad del firmante.
    - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
    - La fecha del acto de aceptación.
    -
- Entregar a la persona física identificada en el certificado con la colaboración del subscriptor (empresa, entidad u organización) y/o Autoridad de Registro, la hoja de aceptación del certificado con los siguientes contenidos mínimos:
    - Información básica acerca del uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de prácticas de confianza aplicable, como sus obligaciones, facultades y responsabilidades
    - Información acerca del certificado.
    - Reconocimiento, por parte del firmante, de disponer de acceso al certificado.
    - Régimen de obligaciones del firmante.
    - Responsabilidad del firmante.
    - Método de imputación exclusiva al firmante, de su clave privada y de sus datos de activación del certificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4.
    - La fecha del acto de aceptación.
- Obtener la firma, escrita o electrónica, de la persona identificada en el certificado. En la opción de la firma electrónica de la aceptación, ésta se realiza por medio de los servicios de la plataforma electrónica existente y se firma con una firma electrónica avanzada.

El suscriptor y/o Autoridad de Registro colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y conserva los citados documentos originales (hojas de

entrega y aceptación), remitiendo copia electrónica a LOGALTY, así como los originales cuando LOGALTY precise de acceso a los mismos. Cuando esta documentación se guarda electrónicamente se realiza por medio de los servicios de la plataforma electrónica existente.

4.4.2 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce con una de estas opciones:

- Mediante la firma escrita de una hoja de aceptación.
- Mediante la firma electrónica de una hoja de aceptación, con una firma electrónica avanzada.
- Mediante el cambio del PIN del certificado.

4.4.3 Publicación del certificado

LOGALTY publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes y siempre que LOGALTY disponga de la autorización de la persona física identificada en el certificado.

4.4.4 Notificación de la emisión a terceros

LOGALTY no realiza ninguna notificación de la emisión a terceras entidades.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el firmante

LOGALTY obliga al firmante a:

- Facilitar a LOGALTY información completa y adecuada, conforme a los requisitos de esta Declaración de prácticas de confianza, en especial en lo relativo al procedimiento de registro.

- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Cuando el certificado funcione juntamente con un QSCD, reconocer su capacidad de producción de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4.
- Comunicar a LOGALTY y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2.
- Dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación o de compromiso de las claves de la CA.

4.5.2 Uso por el suscriptor

4.5.2.1 Obligaciones del suscriptor del certificado

LOGALTY obliga contractualmente al suscriptor a:

- Facilitar a la Entidad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Confianza, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a LOGALTY y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.

  - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
  - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
  - La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación de LOGALTY, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación del prestador de servicios de certificación de LOGALTY, sin permiso previo por escrito.

4.5.2.2 Responsabilidad civil del firmante

LOGALTY obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Confianza.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de protección del control exclusivo de acceso a la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.2.3 Responsabilidad civil del suscriptor de certificado

LOGALTY obliga contractualmente al suscriptor a responsabilizarse de:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de prácticas de confianza.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de protección del control exclusivo de acceso a la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3 Uso por el tercero que confía en certificados

4.5.3.1 Obligaciones del tercero que confía en certificados

LOGALTY obliga al tercero que confía en certificados a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Reconocer que las firmas electrónicas verificadas, producidas en un dispositivo cualificado de creación de firma (QSCD) tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que

el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.

- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería inversa sobre la implantación técnica de los servicios de certificación de LOGALTY, sin permiso previo por escrito.
- No comprometer la seguridad de los servicios de certificación de la LOGALTY, sin permiso previo por escrito.

4.5.3.2 Responsabilidad civil del tercero que confía en certificados

LOGALTY obliga contractualmente al tercero a manifestar:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6 Renovación de certificados

Logalty no realiza renovación de certificados.

4.7 Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.8 Revocación y suspensión de certificados

4.8.1 Causas de revocación de certificados

LOGALTY revoca un certificado cuando concurre alguna de las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:
   a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.
   b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.
2) Circunstancias que afectan a la seguridad de la clave o del certificado:
   a) Compromiso de la clave privada, de la infraestructura o de los sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
   b) Infracción, por LOGALTY, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Confianza.
   c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.
   d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.
   e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.
3) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado:
   a) Finalización de la relación jurídica de prestación de servicios entre LOGALTY y el suscriptor.
   b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado.
   c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción por el suscriptor o por la persona identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y persona identificada en el certificado.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

4) Otras circunstancias:

a) La terminación del servicio de certificación de la Entidad de Certificación de LOGALTY, de acuerdo con lo establecido en la sección 5.8.

b) El uso del certificado que sea dañino y continuado para LOGALTY. En este caso, se considera que un uso es dañino en función de los siguientes criterios:

- La naturaleza y el número de quejas recibidas.
- La identidad de las entidades que presentan las quejas.
- La legislación relevante vigente en cada momento.
- La respuesta del suscriptor o de la persona identificada en el certificado a las quejas recibidas.

4.8.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La persona identificada en el certificado.
- El suscriptor del certificado por medio responsable del servicio de certificación.

4.8.3 Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo a LOGALTY.

La solicitud de revocación puede ser solicitada por medio de la plataforma electrónica existente.

La solicitud de revocación comprenderá la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

La solicitud debe ser autenticada, por LOGALTY, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

LOGALTY podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación[5].

El procedimiento de revocación se puede encontrar en el documento "LGT_revocacionCERT".

En caso de que el destinatario de una solicitud de revocación por parte de una persona física identificada en el certificado fuera la entidad suscriptora, una vez autenticada la solicitud debe remitir una solicitud en este sentido a LOGALTY.

La solicitud de revocación será procesada a su recepción, y se informará al suscriptor y, en su caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado revocado.

LOGALTY no reactiva el certificado una vez ha sido revocado.

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de LOGALTY.

4.8.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, en horario de 24x7 y no será superior a las 24 horas[6].

[5] Ap 6.2.4.a) iii) de ETSI EN 319 411-1

[6] Ap 6.2.4.a) vi) de ETSI EN 319 411-1

4.8.5 Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, en horario de 24x7.

4.8.6 Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se verifica el estado de los certificados es consultando el servicio OCSP de la Entidad de Certificación de LOGALTY en la web siguiente:

- http://ocsp1.logalty.es

El servicio OCSP incluye los certificados caducados en sus respuestas.

4.8.7 Frecuencia de emisión de listas de revocación de certificados (LRCs)

LOGALTY emite una LRC al menos cada 24 horas.

La LRC indica el momento programado de emisión de una nueva LRC, si bien se puede emitir una LRC antes del plazo indicado en la LRC anterior, para reflejar revocaciones.

La LRC mantiene obligatoriamente el certificado revocado o suspendido hasta que expira.

Las CRL no incluyen los certificados caducados en sus respuestas.

4.8.8 Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediato razonable tras su generación, que en ningún caso no supera unos pocos minutos.

4.8.9 Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de LOGALTY, que se encuentra disponible las 24 horas de los 7 días de la semana en el web: https://www.logalty.es/certificateauthority/

Para comprobar la última CRL emitida se debe descargar:

- Logalty Qualified CA G2
    - http://crl1.logalty.es/qualifiedLogaltySubCA02.crl
    - http://crl2.logalty.es/qualifiedLogaltySubCA02.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de LOGALTY, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

LOGALTY suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito[7].

LOGALTY mantiene disponible la información del estado de revocación pasado el período de validez del certificado[8], por medio del servicio OCSP. Esta disponibilidad se mantiene en caso de finalización de los servicios PKI por parte de LOGALTY, transfiriendo esta obligación a otro prestador[9].

4.8.10 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

[7] Ap 6.3.10 de ETSI EN 319 411-2

[8] Ap 6.3.10.b) de ETSI EN 319 411-2

[9] Ap 2.3 del "LGT Plan de cese de servicios PKI"

4.8.11 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de LOGALTY es notificado a todos los participantes en los servicios de certificación, en la medida de lo posible, mediante la publicación de este hecho en la página web de LOGALTY, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.8.12 Causas de suspensión de certificados

Este apartado no aplica a los certificados de autenticación web.

Los certificados de LOGALTY pueden ser suspendidos a partir de las siguientes causas:

- Cuando así sea solicitado por el suscriptor o la persona física identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación sea suficiente pero no se pueda identificar razonablemente al suscriptor o la persona física identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente, aunque se pueda identificar razonablemente al suscriptor o la persona física identificada en el certificado.
- Cuando la documentación requerida en la solicitud de revocación no sea suficiente y tampoco permitan identificar razonablemente al suscripto o la persona física identificada en el certificado r.
- La falta de uso del certificado durante un periodo prolongado de tiempo, conocido previamente.
- Si se sospecha el compromiso de una clave, hasta que éste sea confirmado. En este caso, LOGALTY tiene que asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar su compromiso.

4.8.13 Solicitud de suspensión

Este apartado no aplica a los certificados de autenticación web.

Pueden solicitar la suspensión del certificado:

- La persona física identificada en el certificado.

- El suscriptor del certificado por medio de representantes autorizados.

4.8.14 Procedimientos para la petición de suspensión

Este apartado no aplica a los certificados de autenticación web.

- El usuario accede a un formulario web que se encuentra en la web de LOGALTY.
- Una vez rellenado el formulario con su número y letra de DNI/NIE, se envía una contraseña temporal al correo electrónico con el que el usuario solicitó el certificado.
- El usuario debe confirmar con esa contraseña su solicitud de suspensión.
- Una vez confirmada la solicitud, LOGALTY procede a la suspensión del certificado.

Se informa al suscriptor y, todo caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado suspendido.

4.8.15 Período máximo de suspensión

Este apartado no aplica a los certificados de autenticación web.

El plazo máximo de suspensión será de una semana.

4.9 Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de prácticas de confianza.

LOGALTY puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, en la web https://www.logalty.es/certificateauthority/

4.10.2 Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.10.3 Características opcionales

Sin estipulación.

4.11 Depósito y recuperación de claves

4.11.1 Política y prácticas de depósito y recuperación de claves

LOGALTY no presta servicios de depósito y recuperación de claves.

4.11.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5 Controles de seguridad física, de gestión y de operaciones

5.1 Controles de seguridad física

LOGALTY ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes, generación técnica de los certificados y la gestión del hardware criptográfico.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones donde se producen los certificados bajo la plena responsabilidad de LOGALTY, que la presta desde sus instalaciones de alta seguridad, tanto principales como, en su caso, de operación en contingencia, que son debidamente auditadas de forma periódica.

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso

5.1.1 Localización y construcción de las instalaciones

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta y ubicada en una zona de bajo riesgo de desastres y permite un rápido acceso.

La sala donde se realizan las operaciones criptográficas en el Centro de Proceso de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.

LOGALTY dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos

5.1.2 Acceso físico

LOGALTY dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al RAC) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias de la LOGALTY donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa de LOGALTY a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

En cuanto al acceso a las salas de acceso restringido (como la que alberga el CPD), existe un listado con las personas autorizadas a pedir acceso a las personas de las que dependen

directamente de ellos (ya sean empleados o externos). Este listado se revisa con una periodicidad máxima de 6 meses.

Cualquier intervención de un tercero en el CPD requiere que el área de RIM&DATA CENTRE SHARED SERVICES de Fujitsu conozca previamente el detalle de la intervención y se haya planificado la visita.

Para la planificación de la misma es necesaria la apertura de una solicitud de acceso al CPD en el que se debe detallar:

- Personal que accederá a la sala y rol
- Identificar elementos a los que es necesario acceder (elemento o rack completo en el caso de que sea dedicado)
- Acciones que se van a realizar.
- Fecha de la visita
- Duración.

El registro de la solicitud se realizará de acuerdo a los procedimientos establecidos con cada cliente y registrados en la herramienta de gestión de la actividad que corresponda

Una vez que la visita ha sido aprobada, se procederá a la petición de dos llaves necesarias para poder acceder al CPD y custodiadas por dos grupos diferentes de la compañía, con el objetivo de minimizar los riesgos de acceso indebido.

5.1.3 Electricidad y aire acondicionado

Las instalaciones de LOGALTY disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4 Exposición al agua

Las instalaciones están ubicadas en una zona de bajo riesgo de inundación.

Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Las instalaciones y activos de LOGALTY cuentan con sistemas automáticos de detección y extinción de incendios.

5.1.6 Almacenamiento de soportes

Únicamente personal autorizado tiene acceso a los medios de almacenamiento.

La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Proceso de Datos.

5.1.7 Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, de acuerdo con los estándares de nuestro proveedor Fujitsu.

En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8 Copia de respaldo fuera de las instalaciones

LOGALTY utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro de operaciones, de acuerdo con la política de backup (LSGSIPO001 - Política de backup)

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2 Controles de procedimientos

LOGALTY garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de LOGALTY ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

LOGALTY ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno:** Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA:** responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de backup y mantenimiento de la AC.
- **Administrador de Registro:** Persona responsable de aprobar las peticiones de certificados realizadas por el suscriptor.
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad de LOGALTY. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.
- **Oficial de Registro**: Persona encargada junto al Administrador de Registro de la verificación y aprobación de las peticiones de certificados.
- **Oficial de Revocación**: Responsable de comprobar y aplicar los cambios en el estado de un certificado.

- **Responsable de validación**: Responsable de la comprobación y validación de los datos referentes a los dominios enviados por el solicitante para los certificados de Autenticación Web.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Estas personas realizarán sus funciones basándose en el principio de menor privilegio.

5.2.2 Número de personas por tarea

LOGALTY garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes. Especialmente en la manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3 Identificación y autenticación para cada función

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurará que cada persona realiza las operaciones para las que está asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

5.2.4 Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:

- Emisión y revocación de certificados, y el acceso al depósito.
- Generación, emisión y destrucción de certificados de la Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

5.2.5 Sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:

- Componente/módulo de gestión de la Autoridad de Certificación Subordinada

- Componente/módulo de gestión de la Autoridad de Registro
- Componente/módulo de gestión de solicitudes
- Componente/módulo de gestión de claves (HSM)
- Componente/módulo de bases de datos
- Componente/módulo de gestión de CRL
- Componente/módulo de gestión del servicio de OCSP

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Todo el personal que realiza tareas calificadas como confiables, lleva al menos un año trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.

El personal en puestos de confianza no tiene intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

LOGALTY se asegura de que el personal de registro es confiable para realizar las tareas de registro.

El Administrador de Registro ha realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general, LOGALTY retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.

LOGALTY no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación **hasta donde permita la legislación aplicable**, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.

- Morosidad.

5.3.2 Procedimientos de investigación de historial

LOGALTY, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

LOGALTY realiza dichas comprobaciones con observancia estricta del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

5.3.3 Requisitos de formación

LOGALTY forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.

Los programas de formación son actualizados y mejorados de forma periódica.

La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad de LOGALTY. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4 Requisitos y frecuencia de actualización formativa

LOGALTY actualiza la formación del personal de acuerdo con las necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

LOGALTY dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por LOGALTY. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante, lo cual, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por tercero distinto a LOGALTY.

5.3.8 Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4 Procedimientos de auditoría de seguridad

LOGALTY está sujeta a las validaciones cada dos años por medio de auditorías LOPD. Además dispone de una auditoría anual de revisión de seguridad con el objetivo de identificar y analizar las vulnerabilidades potencialmente explotables.

5.4.1 Tipos de eventos registrados

LOGALTY produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.

- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.
- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación de este.
- Las actividades de los cortafuegos y enrutadores[10]
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.

Las entradas del registro incluyen los siguientes elementos:

- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

[10] Ap 6.4.5.a) de ETSI EN 319 411-1

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas que son usados por los firmantes o custodios[11].

5.4.2 Frecuencia de tratamiento de registros de auditoría

LOGALTY revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.

El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.

LOGALTY mantiene un sistema que permite garantizar:

- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3 Período de conservación de registros de auditoría

LOGALTY almacena la información de los logs al menos durante 15 años.

5.4.4 Protección de los registros de auditoría

Los logs de los sistemas:

- Están protegidos de manipulación, borrado o eliminación[12] mediante la firma de los ficheros que los contienen.

[11] Ap 6.4.5.a) de ETSI EN 319 411-2

[12] Ap 7.10.f) de ETSI EN 319 401

- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.

El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado.

Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5 Procedimientos de copia de respaldo

LOGALTY dispone de un procedimiento adecuado de backup de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

LOGALTY tiene implementado un procedimiento de backup seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6 Localización del sistema de acumulación de registros de auditoría

La información de la auditoria de eventos es recogida automáticamente por el sistema operativo, las comunicaciones de red y por el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

5.4.8 Análisis de vulnerabilidades

El análisis de vulnerabilidades queda cubierto por los procesos de auditoría de LOGALTY.

Los análisis de vulnerabilidad deben ser ejecutados, repasadas y revisadas por medio de un examen de estos acontecimientos monitorizados. Estos análisis deben ser ejecutados cada día, cada mes y cada año.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

5.5 Archivos de informaciones

LOGALTY, garantiza que toda la información relativa a los certificados se conserva durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1 Tipos de registros archivados

Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por LOGALTY (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y su ubicación
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación.
- Todas aquellas elecciones específicas que el firmante o el subscriptor disponga durante el acuerdo de subscripción[13].
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.
- El historial de claves generadas.
- Las comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación

[13] Ap 6.4.5.c) iv) de ETSI EN 319 411-1

- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

LOGALTY es responsable del correcto archivo de todo este material.

5.5.2 Período de conservación de registros

LOGALTY archiva los registros especificados anteriormente durante 15 años.

5.5.3 Protección del archivo

LOGALTY protege el archivo de forma que sólo personas debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

LOGALTY asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

5.5.4 Procedimientos de copia de respaldo

LOGALTY dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

LOGALTY como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realiza copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, LOGALTY (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

5.5.5 Requisitos de sellado de fecha y hora

Los registros están fechados con una fuente fiable vía NTP con conexión a Fujitsu.

Los servidores de LOGALTY están conectados a una ip virtual de Fujitsu (193.148.29.99) que a su vez está conectado contra el servidor NTP de stratum 1 de RedIris (hora.rediris.es), que está situado en la Universidad Autónoma de Madrid.

La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día[14].

No es necesario que esta información se encuentre firmada digitalmente.

5.5.6 Localización del sistema de archivo

LOGALTY dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos de obtención y verificación de información de archivo

LOGALTY dispone de un procedimiento donde se describe el proceso para verificar que la información archivada es correcta y accesible.

5.6 Renovación de claves

Con anterioridad a que el uso de la clave privada de la AC caduque, será realizado un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN.

El cambio de claves del suscriptor es realizado mediante la realización de un nuevo proceso de emisión.

5.7 Compromiso de claves y recuperación de desastre

[14] Ap 7.10.d) de la ETSI EN 319 401

5.7.1 Procedimientos de gestión de incidencias y compromisos

Son almacenadas copias de seguridad de la siguiente información en instalaciones de almacenamiento externo a LOGALTY, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de LOGALTY son generadas y mantenidas de acuerdo con lo establecido en la sección 6.2.4

5.7.2 Corrupción de recursos, aplicaciones o datos

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres de LOGALTY.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de LOGALTY, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación, desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Certificación.

En caso de compromiso de la clave privada de LOGALTY puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos[15]. LOGALTY ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario (LGT Plan de Continuidad PKI_v1.0).

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio

[15] Ap 6.4.8.g) ii) de ETSI EN 319 411-1

tratará los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

5.7.4 Continuidad del negocio después de un desastre

LOGALTY restablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con el plan de contingencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.

LOGALTY dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

5.8 Terminación del servicio

LOGALTY asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, LOGALTY desarrolla un plan de terminación, con las siguientes provisiones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.
- Informará a todos Firmantes/Suscriptores, Tercero que confían y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.

- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Comunicará al Ministerio de Industria, Energía y Turismo, con una antelación mínima de 2 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también al Ministerio de Industria, Energía y Turismo, la apertura de cualquier proceso concursal que se siga contra LOGALTY, así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6 Controles de seguridad técnica

LOGALTY emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de la entidad de certificación intermedia "LOGALTY QUALIFIED CA G2" es creado por la entidad de certificación raíz "LOGALTY CA ROOT 03" de acuerdo con los procedimientos de ceremonia de LOGALTY, dentro del perímetro de alta seguridad destinado a esta tarea.

Las actividades realizadas durante la ceremonia de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en la misma, con la presencia de un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por LOGALTY.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140 2, Common Criteria EAL4+ certified y conforme a CWA/ETSI

Entidad Raíz "LOGALTY CA ROOT 03"	**4.096 bits**	**25 años**
Entidad Subordinada "LOGALTY QUALIFIED CA G2"	4.096 bits	13 años
- Certificados de entidad final	2.048 bits	3 años
Unidad de Sello de Tiempo	4.096 bits	6 años

Más información en la ubicación:

https://www.logalty.es/certificateauthority/

6.1.1.1 Generación del par de claves del firmante

Las claves del firmante son creadas por él mismo mediante software o hardware autorizados por LOGALTY.

Las claves son generadas usando el algoritmo de clave pública RSA, con una longitud mínima de 2048 bits.

6.1.2 Envío de la clave privada al firmante

En certificados en dispositivo cualificado de creación de firma la clave privada se encuentra debidamente protegida en el interior de dicho dispositivo seguro.

En certificados en software centralizados, la clave privada del firmante se crea en el dispositivo cualificado de creación de firma y bajo el exclusivo control del titular se gestiona desde la plataforma Nebulacert.

En certificados en software distribuidos la clave privada del firmante se crea en el sistema informático que utiliza este firmante cuando realiza la solicitud del certificado, por lo que no existe envío de clave privada.

6.1.3 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS#10, otra prueba criptográfica equivalente o cualquier otro método aprobado por LOGALTY.

Cuando las claves se generan en un QSCD, LOGALTY se asegura que la clave pública que se remite al prestador de servicios de certificación proviene de un par de claves generadas por dicho QSCD[16].

6.1.4 Distribución de la clave pública del prestador de servicios de certificación

Las claves de LOGALTY son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

[16] Ap 6.5.1.b) de ETSI EN 319 411-2

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de las CA raíz y subordinadas estarán a disposición de los usuarios en la página Web de LOGALTY.

6.1.5 Tamaños de claves

La longitud de las claves de la Entidad de Certificación raíz o subordinadas es de 4096 bits como mínimo.

Las claves de los certificados de entidad final son de 2048 bits.

6.1.6 Generación de parámetros de clave pública

La clave pública de la CA Root, de la CA subordinadas y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

6.1.7 Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096
- Funciones criptográficas de Resumen: SHA512WithRSA.

6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9 Propósitos de uso de claves

Los usos de las claves para los certificados de las CA son exclusivamente para la firma de certificados y de CRLs.

Los usos de las claves para los certificados de entidad final para personas físicas son exclusivamente para la firma digital y el no repudio.

Los usos de las claves para los certificados de entidad final para sellos electrónicos son exclusivamente para la firma digital, el no repudio y el cifrado.

6.2 Protección de la clave privada

6.2.1 Estándares de módulos criptográficos

En relación con los módulos que gestionan claves de LOGALTY y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

6.2.2 Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de **2 de 3** personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

6.2.3 Depósito de la clave privada

LOGALTY no almacena copias de las claves privadas de los firmantes.

6.2.4 Copia de respaldo de la clave privada

LOGALTY realiza copia de backup de las claves privadas de las CA que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación

de la copia como la recuperación de ésta necesitan al menos de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del suscriptor en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación.

Las claves del firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

6.2.5 Archivo de la clave privada

Las claves privadas de las AC son archivadas por un periodo de **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de LOGALTY.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

6.2.7.1 Almacenamiento de la clave privada de las Autoridades de Certificación

Las claves privadas de la Entidad de Certificación se almacenan cifradas en los módulos criptográficos de producción de LOGALTY.

6.2.7.2 Almacenamiento de la clave privada del firmante

Las claves privadas para la firma electrónica cualificada y el sello electrónico cualificado se generan exclusivamente en el hardware criptográfico dispuesto para esta función desde la entrada en funcionamiento en LOGALTY de la plataforma electrónica NebulaSuite[17]

Las claves privadas para la firma electrónica avanzada y el sello electrónico avanzado se almacenan en el hardware criptográfico.

En ningún caso resulta posible proceder a la importación de claves privadas de firma electrónica cualificada o sello electrónico cualificado en NebulaSuite.

De esta forma se da cumplimiento al artículo 26.c) del Reglamento UE 910/2014 que indica que las firmas electrónicas avanzadas deben "haber sido creadas utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo," y al artículo 36.c) del Reglamento UE 910/2014 que indica que los sellos electrónicos avanzados deben "haber sido creados utilizando datos de creación del sello electrónico que el creador del sello puede utilizar, con un alto nivel de confianza, bajo su control exclusivo".

Asimismo, y para el caso de la firma electrónica cualificada, la generación de las claves por parte del prestador cualificado permite cumplir el considerando 51 del Reglamento UE 910/2014 que indica que debe ser posible para el firmante confiar a un tercero los dispositivos cualificados de creación de firmas electrónicas a condición de que se apliquen los procedimientos y mecanismos adecuados para garantizar que el firmante tiene el control exclusivo del uso de sus datos de creación de la firma electrónica y que la utilización del dispositivo cumple los requisitos de la firma electrónica cualificada.

Finalmente este entorno fiable de generación de las claves da cumplimiento a la generación de los datos de creación de firma en nombre del firmante indicado en el artículo 18.a) de la Ley 59/2003 de firma electrónica.

[17] Ver apartado 1.3.1.3 "NEBULACert"

6.2.8 Método de activación de la clave privada

La clave privada de LOGALTY se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

Las claves de la AC se activan por un proceso de m de n (2 de 3)

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC.

6.2.9 Método de desactivación de la clave privada

Para la desactivación de la clave privada de LOGALTY se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente.

Por su parte el firmante deberá introducir el PIN para la nueva activación.

6.2.10 Método de destrucción de la clave privada

Con anterioridad a la destrucción de las claves, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas de LOGALTY. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

Finalmente se destruirán de forma segura las copias de seguridad.

Las claves del firmante en software se podrán destruir mediante el borrado de las mismas, siguiendo las instrucciones de la aplicación que las alberga.

Las claves del firmante en hardware podrán ser destruidas mediante una aplicación informática especial en las dependencias de las RA o de LOGALTY.

6.2.11 Clasificación de módulos criptográficos

Ver la sección 6.2.1

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

LOGALTY archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de este documento.

6.3.2 Períodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de LOGALTY son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves.

La creación y distribución de dichos dispositivos es registrada.

Asimismo, LOGALTY genera de forma segura los datos de activación.

6.4.2 Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de las Autoridades de certificación raíz y subordinadas, son protegidos por los poseedores de las tarjetas de administradores de los módulos criptográficos, según consta en el documento de ceremonia de claves.

El firmante del certificado es el responsable de la protección de su clave privada, con una contraseña lo más completa posible. El firmante debe recordar dicha contraseña.

6.5 Controles de seguridad informática

LOGALTY emplea sistemas fiables para ofrecer sus servicios de certificación. LOGALTY ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuados con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, LOGALTY sigue el esquema de certificación sobre sistemas de gestión de la información ISO 27001.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas de LOGALTY, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de Log.
- Plan de backup y recuperación.
- Configuración antivirus.
- Requerimientos de trafico de red.

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor de LOGALTY incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la SubCA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y la SubCA y datos de auditoria.
- Auditoria de eventos relativos a la seguridad.
- Autodiagnóstico de seguridad relacionado con los servicios de la SubCA.
- Mecanismos de recuperación de claves y del sistema de la SubCA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

La verificación de la certificación de los dispositivos cualificados (QSCD) se realiza durante todo el período de validez del certificado[18]. Si el QSCD perdiera su certificación como tal, LOGALTY avisará a los usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por LOGALTY son fiables.

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por LOGALTY de acuerdo con estándares de desarrollo y control de cambios.

Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2 Controles de gestión de seguridad

LOGALTY desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad. En la realización de esta función dispone de un plan de formación anual.

[18] Ap 6.5.1.c) de ETSI EN 319 411-2

LOGALTY exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.1 Clasificación y gestión de información y bienes

LOGALTY mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de LOGALTY detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: SIN CLASIFICAR, USO INTERNO, y CONFIDENCIAL.

6.6.2.2 Operaciones de gestión

LOGALTY dispone de un procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos (Logalty ProcIT-DSS02 Gestión de peticiones e incidencias v2r1).

En el documento de seguridad de LOGALTY se desarrolla en detalle el proceso de gestión de incidencias.

LOGALTY tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

6.6.2.3 Tratamiento de los soportes y seguridad

Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

6.6.2.3.1 Planificación del sistema

El departamento de Sistemas de LOGALTY mantiene un registro de las capacidades de los equipos. Juntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

6.6.2.3.2 Reportes de incidencias y respuesta

LOGALTY dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

6.6.2.3.3 Procedimientos operacionales y responsabilidades

LOGALTY define actividades, asignadas a personas con un rol de confianza, distintas de las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.4 Gestión del sistema de acceso

LOGALTY realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.

En particular:

6.6.2.4.1 AC General

- Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.
- Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.
- LOGALTY dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.
- LOGALTY dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.
- Cada persona tiene asociado un rol para realizar las operaciones de certificación.
- El personal de LOGALTY es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

6.6.2.4.2 Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de LOGALTY.

6.6.2.4.3 Gestión de la revocación

La revocación se realizará mediante autenticación fuerte a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de LOGALTY.

6.6.2.4.4 Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación con certificados o con doble factor de identificación para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.5 Gestión del ciclo de vida del hardware criptográfico

LOGALTY se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.

LOGALTY registra toda la información pertinente del dispositivo para añadir al catálogo de activos.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

LOGALTY realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo hardware criptográfico solo es manipulado por personal confiable.

La clave privada de firma de LOGALTY almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de LOGALTY, así como sus modificaciones y actualizaciones son documentadas y controladas.

LOGALTY posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7 Controles de seguridad de red

LOGALTY protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8 Controles de ingeniería de módulos criptográficos

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.

Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.

Todas las operaciones criptográficas de LOGALTY son realizadas en módulos con las certificaciones FIPS 140 level 3 y/o Common Criteria EAL 4+ (con la aumentación ALC_FLR.1).

6.9 Fuentes de Tiempo

LOGALTY tiene un procedimiento de sincronización de tiempo coordinado con Fujitsu vía NTP.

Los servidores están conectados a una ip virtual de Fujitsu (193.148.29.99) que a su vez está conectado contra el servidor NTP de stratum 1 de RedIris (hora.rediris.es), situado en la Universidad Autónoma de Madrid.

7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

Todos los certificados cualificados emitidos bajo esta política cumplen el estándar X.509 versión 3, RFC 3739 y ETSI 101 862 “Qualified Certificate Profile”.

7.1.1 Número de versión

LOGALTY emite certificados X.509 Versión 3

7.1.2 Extensiones del certificado

Las extensiones de los certificados se encuentran detalladas en los documentos de perfiles que son accesibles desde la página web de LOGALTY https://www.logalty.es/certificateauthority/

De esta forma se permite mantener unas versiones más estables de la DPC desligándolas de los frecuentes ajustes en los perfiles.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5 Restricción de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos.

Adicionalmente se pueden establecer restricciones de nombres en relación con los certificados en la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica, siempre que las mismas resulten objetivas, proporcionadas, transparentes y no discriminatorias.

7.1.6 Identificador de objeto (OID) de los tipos de certificados

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos, de acuerdo con la estructura indicada en el punto 1.2.1

7.2 Perfil de la lista de revocación de certificados

7.2.1 Número de versión

Las CRL emitidas por LOGALTY son de la versión 2.

7.2.2 Perfil de OCSP

Según el estándar IETF RFC 6960

8 Auditoría de conformidad

Logalty realiza auditorías de conformidad para asegurar el cumplimiento y adecuación con las políticas, normativas, planes y procedimientos de seguridad del sistema de gestión de seguridad de la información. Dichas auditorías, su alcance y periodicidad, se describen en el correspondiente Plan de Auditoría de Logalty, que se actualiza de forma anual. Como resultado de las mismas se elaboran planes de acciones correctivas como respuesta a la nos conformidades y desviaciones detectadas.

Logalty realiza las pertinentes auditorías de conformidad del Reglamento eIDAS por medio de evaluaciones de conformidad bianuales de las normas ETSI EN 319 401, ETSI EN 319 411-1 y ETSI EN 319 411-2.

Logalty realiza las pertinentes auditorías sobre protección de datos con periodicidad bianual.

8.1 Frecuencia de la auditoría de conformidad

LOGALTY realiza evaluaciones de conformidad eIDAS con carácter bienal, además de revisiones anuales.

LOGALTY realiza auditorías RGPD bianuales, con revisiones anuales.

LOGALTY realiza análisis de vulnerabilidades cada 3 meses

LOGALTY realiza un análisis de intrusión cada 6 meses

8.2 Identificación y calificación del auditor

Las auditorías son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

El auditor responsable de la evaluación de conformidad Eidas debe estar acreditado según ETSI EN 319 403.

Para la evaluación de conformidad eIDAS Logalty ha usado los servicios de AENOR (https://www.aenor.com/)

8.3 Relación del auditor con la entidad auditada

Los auditores internos o externos responsables de ejecutar las auditorías son independientes funcionalmente del servicio de producción objeto de auditoría.

8.4 Listado de elementos objeto de auditoría

La auditoría verifica respecto a LOGALTY:

a) Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
b) Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales, bajo el marco del Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014.
c) Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por LOGALTY y con lo establecido en la normativa vigente.
d) Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

a) Procesos de la AC, ARs y elementos relacionados.
b) Sistemas de información.
c) Protección del centro de proceso de datos.
d) Documentación asociada.

8.5 Acciones que emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento realizada, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si la Entidad de Certificación de LOGALTY es incapaz de desarrollar y/o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema, deberá comunicarlo inmediatamente al Comité de Seguridad de la Información de LOGALTY que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la AC y regenerar la infraestructura.
- Terminar el servicio de la AC.
- Otras acciones complementarias que resulten necesarias.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Comité de Seguridad de la Información de LOGALTY en un plazo máximo de 15 días tras la ejecución de la auditoría, para su análisis y tratamiento.

Si a causa de la auditoría realizada fuera necesaria la revocación de certificados, este informe servirà como justificante de dicha revocación.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

LOGALTY puede establecer una tarifa por la emisión o por la renovación de los certificados, de la que, en su caso, se informará oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a certificados

LOGALTY no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

LOGALTY no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación.

9.1.5 Política de reintegro

Sin estipulación.

9.2 Capacidad financiera

LOGALTY dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y

perjuicios, según lo establecido en la ETSI EN 319 401-1 7.12 c), en relación con la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

LOGALTY dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014 con un mínimo asegurado de 3.000.000 de euros.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados

LOGALTY dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014, con un mínimo asegurado de 3.000.000 de euros.

9.3 Confidencialidad

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por LOGALTY:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.

- Registros de auditoría interna y externa, creados y/o mantenidos por la Entidad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2 Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Entidad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor, en el supuesto de que sea significativa en función de la finalidad del certificado.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier otra información que no esté indicada en la sección anterior.

9.3.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

LOGALTY divulga la información confidencial únicamente en los casos legalmente previstos.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa[19], serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

La Entidad de Certificación indicará estas circunstancias en la política de privacidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

LOGALTY incluye, en la política de privacidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de datos personales

Para la prestación del servicio, LOGALTY precisa recabar y almacenar ciertas informaciones, que incluyen datos personales. Tales informaciones son recabadas a través de los suscriptores, en base a la relación corporativa que les une con los poseedores de claves (empleados, cargos, socios…), o en ciertos casos, directamente de los afectados, con cumplimiento estricto de las

[19] Apartado 7.10.c) de la ETSI EN 319 401

condiciones para el tratamiento legítimo a que se refiere el artículo 6 Reglamento general de protección de datos.

LOGALTY recaba los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.

LOGALTY ha desarrollado una política de privacidad y documentado en esta Declaración de Prácticas de Confianza los aspectos y procedimientos de seguridad correspondientes de conformidad con el Reglamento general de protección de datos.

LOGALTY no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8 del presente documento, en caso de terminación del servicio de certificación.

La información confidencial de acuerdo con la normativa en protección de datos personales se protege de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de conformidad con las prescripciones establecidas en este documento en cumplimiento del Reglamento general de protección de datos.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

Únicamente LOGALTY goza de derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de los derechos de los suscriptores, poseedores de claves y terceros, a los que conceda licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por LOGALTY contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2 Propiedad de la Declaración de prácticas de confianza

Únicamente LOGALTY goza de derechos de propiedad intelectual sobre esta Declaración de prácticas de confianza.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado conserva la totalidad de derechos, de existir los mismos, sobre la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1.1 del presente documento.

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los firmantes, las personas físicas que poseen de forma exclusiva las claves de firma digital.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de la Entidad de Certificación de LOGALTY

LOGALTY garantiza, bajo su plena responsabilidad, que cumple con la totalidad de los requisitos establecidos en la DPC, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso si una parte o la totalidad de las operaciones se subcontratan externamente.

LOGALTY presta los servicios de certificación conforme con esta Declaración de prácticas de confianza.

Con anterioridad de la emisión y entrega del certificado al suscriptor, LOGALTY informa al suscriptor de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso, mediante un contrato de suscriptor.

Este requisito de información también se cumple mediante un documento PDS[20], también denominado texto de divulgación, que incorpora el contenido del anexo A de la normat técnica ETSI EN 319 411-1 v1.1.1 (2016-02), documento que puede ser transmitido por medios electrónicos, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

LOGALTY comunica de forma permanente los cambios[21] que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://www.logalty.es/certificateauthority/, a suscriptores, poseedores de claves y terceros que confían en certificados mediante dicho PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.2, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Entidad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Entidad de Certificación acepta o excluye su responsabilidad.

[20] "PKI Disclosure Statement", o declaración de divulgación de PKI aplicable.

[21] Ap 6.2.3.b) de ETSI EN 319 411-1

- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

LOGALTY, en la documentación que la vincula con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

LOGALTY, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la Declaración de prácticas de confianza.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de prácticas de confianza.

LOGALTY, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de prácticas de confianza.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, LOGALTY garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo I del Reglamento (UE) 910/2014.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan.

9.6.3 Rechazo de otras garantías

LOGALTY rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4 Limitación de responsabilidades

LOGALTY limita su responsabilidad a la emisión y gestión de certificados y de pares de claves de suscriptores suministrados por la Entidad de Certificación.

9.6.5 Cláusulas de indemnidad

9.6.5.1 Cláusula de indemnidad de suscriptor

LOGALTY incluye en el contrato con el suscriptor, una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.

- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión ha mediado dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2 Cláusula de indemnidad de tercero que confía en el certificado

LOGALTY incluye en el PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6 Caso fortuito y fuerza mayor

LOGALTY incluye en el PDS cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.6.7 Ley aplicable

La Entidad de Certificación establece, en el contrato de suscriptor y en el PDS, que la legislación aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

9.6.8 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

LOGALTY establece, en el contrato de suscriptor, y en el PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9 Cláusula de jurisdicción competente

LOGALTY establece, en el contrato de suscriptor y en el PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10 Resolución de conflictos

LOGALTY establece, en el contrato de suscriptor, y en el PDS, los procedimientos de mediación y resolución de conflictos aplicables.